From:	Moody, Dustin (Fed)
To:	Alperin-Sheriff, Jacob (Fed)
Subject:	FW: Can I Go Ahead and Ask the PQC forum to let us know whether there are any other "MUST-HAVE" libraries we should
Date:	Tuesday, July 25, 2017 2:23:00 PM

Go ahead then. Perhaps send us your message before you post.

From: Bassham, Lawrence E (Fed)
Sent: Tuesday, July 25, 2017 2:22 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Can I Go Ahead and Ask the PQC forum to let us know whether there are any other "MUST-HAVE" libraries we should

Murugiah wants to discuss next Tuesday when he's back. I don't think it hurts to get started on the list of libraries now.

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, July 25, 2017 at 2:17 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Can I Go Ahead and Ask the PQC forum to let us know whether there are any other "MUST-HAVE" libraries we should

I don't think it hurts to wait a day or two to see if Larry gets an answer, and then we can give a much better explanation on the forum.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, July 25, 2017 2:16 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Can I Go Ahead and Ask the PQC forum to let us know whether there are any other "MUST-HAVE" libraries we should

consider guaranteeing (in a specific install directory and with a specific version of said library) will already be available on our reference platforms (besides GMP and NTL, which I already figure are "MUST-HAVE")?

Or are we waiting on Larry and that VM idea?

—Jacob Alperin-Sheriff